

Smart Society: How to Trust Digital Intelligence

Smart societies are our future. There will be more smart devices than the human population, by the end of 2050. The human machine interaction is predicted to grow exponentially. All the data will go digital and there will be a central repository, with uniform protocols and modes of access. Thus, it becomes imperative that **digital intelligence systems**, responsible for handling, accessing, storing and keeping data safe are designed in the most secure and robust way possible. Ideally, the technology must be easy to use and maintain, safe from tampering and invasion, easily scalable according to demand and adaptable to changes. It is necessary to use cryptographic models that are apt, for ciphering and encryption of data. It is encouraged to use digital signatures or fingerprints for important documents. Technical and legal professionals work to ensure that the necessary electronic data is identified and preserved.

Today, digital forensics have evolved enough to ensure that electronic frauds are detected and prevented. It works in tandem with the cyber crime branch to make sure that electronic data is safe over the internet and attack free. Authentication methods are designed effectively to detect unauthorized login attempts. Consultants provide counsel about the handling of data.

Storage systems have evolved, given that virtual storage machines and cloud computing are operating at their optimal

best. Data can be accessed anytime and anywhere on demand, giving complete freedom to the user.

With the evolution of connected devices and internet of things (IoT), that power a connected society, it becomes increasingly important to prevent hacking of WiFi networks and to protect sensitive information sent over applications and networks. Suspicious users, websites and IP addresses need to be identified and blocked from accessing important information over the network. A dedicated team needs to be set up to prevent age old threats like trojans, viruses, DoS attacks, phishing and malware.

If Voice over Internet Protocol (VoIP) is implemented, care needs to be taken that the call servers and the telephony infrastructure components are always running optimally, balancing call loads and trunking. Another important aspect of the digital intelligence infrastructure is scalability. As and when new users join or old users quit the network, the system must be capable of scaling up and down, according to the demand and make the on-boarding and off-boarding process easy.

As and when new technologies are implemented and the system is upgraded, the software and hardware must be able to adapt well and not lose momentum while operating. Software experts will have to work on updating to latest versions, enhancing features, making patches, making code bug free and ensuring it

runs efficiently. Today, we have many tools at our disposal : **housing society management system software, visitor management software** for better safety and connectivity in the **visitor management** domain and **residential management systems**, to empower every household. Such technologies have sprung up in **Pune** and in many other IT hubs of **India**.

To be able to achieve a highly trustworthy digital intelligence system, experimentation, research and development has to be fostered. Opportunities can be given to freelancers and full time professionals alike. Academicians can provide their valuable inputs through research. It is important that the community ideates, discusses and implements continuous tests to improve the system and its performance. It's important that the standard and best practices are used for the same.